UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/566,393	01/27/2006	Junbiao Zhang	PU030228	3745

24498 7590 06/04/2010

Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER	
SIMS, JING F	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
06/04/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/566,393	ZHANG, JUNBIAO	
	Examiner	Art Unit	
	JING SIMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,25-34,36 and 41-57* is/are pending in the application.

4a) Of the above claim(s) *14-24,35 and 37-40* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,25-27,34,36 and 41-57* is/are rejected.

7)☐ Claim(s) *28-33* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 2/12/2010, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437.

Response to Arguments

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

3. In response to applicant's argument to claims 54 and 56 that the references fail to show certain features of applicant's invention, it is noted that the features upon which

applicant relies (i.e., "generating a web page requesting authentication information") are not recited in the rejected claims 54 and 56. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4. Applicant argued the rejection to claim 42 as "Claxton et al does not generate a local digital signature; rather, Claxton et al regenerates signature" on page 16, last paragraph. Examiner respectfully disagrees. In light of the instant specification, digital signature is generated the first time (page 9, line 2), and generated again for comparison with the digital signature that generated first time (page 9, lines 17-20: "following the same method that was used by AS in generating digital signature "g""); thus, in the instant application the signature is regenerated by different entity. Claxton discloses RM regenerates signature by public key sent from client (in col. 51, lines 28-30) in order to compare with the signature generated by authentication server which disclosed in the background section (col. 1, lines 60-67 to col. 2, lines 1-9); Therefore Claxton teaches the corresponding limitations in claim 42.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 54-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US 5708780, hereinafter Levergood) in view of Peiffer et al (US patent application pub. no.: 2003/0037108).

As per claim 54, Levergood discloses a method for controlling network access *(col. 3, lines 8-9, methods of processing service requests from a client to a server through a network)*, said method comprising:

receiving an authentication user input message *(col. 6, lines 36-41, authentication server receives a request from client)*;

transmitting authentication input page requesting authentication information *(col. 6, lines 44-49, authentication server sends a challenge response which causes the client browser to prompt the user for credentials; a preferred credential query typically consists of a request for user name and password)*;

receiving authentication credentials *(col. 6, lines 58-66, upon receiving the get request)*; and

transmitting an authentication message indicating one of success and failure of an authentication process *(col. 6, lines 58-66, and col. 7, lines 1-20, if the user is not cleared for authorization, a page denying access 222 is transmitted to the client browser. If the user is qualified, the new user is sent a form page)*.

As per claim 55, claim 54 is incorporated and Levergood discloses:

wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number *(col. 6, lines 5-16, the authentication request get URL contains a SID, and User IP. From lines 54 to 64,*

Levergood teaches that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. User IP is considered as session identifier. Since the SID is encoded the data it includes a random number).

Claims 56-57 are system claims corresponding to the method claims 54-55 and therefore are rejected under the same reasons set forth in the rejections for claims 54-55.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 48-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US 5708780, hereinafter Levergood) in view of Peiffer et al (US patent application pub. no.: 2003/0037108).

As per claim 48, Levergood discloses a method for controlling network access *(col. 3, lines 8-9, methods of processing service requests from a client to a server through a network)*, said method comprising:

receiving a re-directed request for network access via a message *(col. 3, lines 27-29, content server initiates the authorization routine by redirecting the client's request to an authentication server)*;

transmitting a client identifier and unique data *(col. 5, lines 49-65, an SID provided from the authentication server to the client. The SID includes 22-bit user identifier, and other specific data; wherein 22-bit user identifier correspond with client identifier; other data, such as 32-bit signature correspond with unique data)*;

Levergood does not disclose generating a web page including embedded data.

Peiffer discloses:

generating a web page including embedded data *(par. [0058], lines 7-10, server is configured to recognize the SSID and generate a customized web resource A, shown in at 30c; wherein web resource A corresponding with webpage; lines 14-19, the links in the customized web resource A are rewritten to include the SID, wherein the SID corresponding with embedded data).*

Levergood and Peiffer are analogous art because they are from the same field of endeavor of secure network accessing.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the Internet server control system as described by Levergood and add generating a customized webpage for the client as taught by Peiffer because it would maintain a stateful interactions between clients and service provider (see Peiffer, par. [0010]).

As per claim 49, claim 48 is incorporated and Levergood discloses:

wherein said unique data comprises a session identifier and a random number *(col. 5, lines 54-65, wherein 16-bit expiration date, and/or 2-bit key identifier, and or 8-bit domain correspond with session identifier; the digital signature which is a cryptographic hash of the remaining items in the SID correspond with a random number)*.

As per claim 50, claim 48 is incorporated and Levergood discloses:

wherein said embedded data comprises a session identifier, a random number and authentication server selection information (col. 5, lines 48-65, wherein a modified URL appended with an SID correspond with embedded data; 1-bit expiration data, *and/or 2-bit key identifier, and or 8-bit domain correspond with session identifier; the digital signature which is a cryptographic hash of the remaining items in the SID correspond with a random number; the authorized IP address correspond with authentication server selection information)*.

Claims 51-53 are system claims corresponding to the method claims 48-50 and therefore are rejected under the same reasons set forth in the rejections for claims 48-50.

7. Claims 1-2, 6, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Neill (US 2004/0047348) in view of Jones et al (US 2003/0212800, hereinafter Jones), and further in view of Peiffer.

As per claim 1, O'Neill discloses a method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client *(fig. 11,and [0048], wherein mobile node*

MN 910 correspond with the client, first Access Node FA 920 corresponding with access point, AP);

re-directing, by said AP, said access request to a local server *(fig. 11, and [0049], wherein First Home Agent HA 930 correspond with Local server; process 970b correspond with re-directing)*;

associating unique data with an identifier of said client and storing a mapping of said association in said AP *(fig. 11, and [0047], wherein binding table 933 correspond with associating, the MIP related to End Node 910 correspond with identifier of said client, and Host Home Address HoA correspond with Unique data)*;

transmitting an authentication request to said selected authentication server *(fig. 11,and [0048], send a message 906a to AAA, Authentication, Authorization and Accounting, server 905; wherein RADIUS access_request to the AAA system 905 correspond with authentication request)*; and

receiving a response to said authentication request from said selected authentication server *(fig. 11,and [0048], a multitude of Policy state to be returned to F A 920 proves the authentication request has been received at RADIUS server).*

However, O'Neill does not disclose:

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client;

Jones discloses:

Hosting **a web page by said local server requesting that said client select an authentication server (AS)** *(page 5, [0059], wherein web server 114 corresponding with local server, authentication-invite web page corresponding with web page; [0060], web page can include a field for a user to select a service provider from among those available)* **and including said unique data and forwarding the web page to said client** *([0060], wherein SIP address, password, and/or other credentials correspond with unique data).*

O'Neill and Jones are analogous art because they are from the same field of endeavor of wireless communication access control.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the verification process of a mobile node as described by O'Neill and add giving user options to select a service provider as taught by Jones because it would provide mobile device user an other choice to connection to Internet while in the range of an hot spot.

Jones discloses hosting an authentication-invite webpage requesting client select an authentication server; however, Jones does not disclose generating the webpage, and forwarding said generated web page to said client.

Peiffer discloses **generating a webpage** *(par. [0058], the server is configured to recognize the SSID and generate a customized web resource A, based on the user's past behavior associated with the SSID).*

O'Neill, Jones, and Peiffer are analogous art because they are from the same field of endeavor of network access controlling.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify hosting the authentication-invite web page stored at the server as described by Jones to be generated at the server based receiving information as taught by Peiffer because it would provide customized web resource for client's request (see Peiffer, par. [0058], lines 14-19).

As per claim 2, claim 1 is incorporated and O'Neill discloses:

wherein said network is a wireless Local Area network (WLAN) *(fig. 11 and [0002], mobile communications)*.

As per claim 6, claim 1 is incorporated and O'Neill discloses:

wherein said identifier is an address of said client *(fig. 11, and [0047], MIP is mobile IP which is an address of an end note/user)*.

As per claim 10, claim 1 is incorporated and O'Neill discloses:

wherein said identifier is one of a physical (PHY) address of said client, a MAC address of said client and an IP address of said client *(fig. 11, and [0047], MIP is mobile IP of an end note/user)*.

8. Claims 1, 3-5, 7-9, 11-13, 34, 36, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood et al. (US 5708780) (hereinafter Levergood) in view of Stewart et al. (US 6732176) (hereinafter Stewart), and further in view of Jones, and further in view of Peiffer.

As per claims 1, Levergood discloses a method for controlling access to a network, said method comprising *(col. 3, lines 8-9, methods of processing service requests from a client to a server through a network)*:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client *(col. 3, lines 8-29, with respect to this limitation, Levergood discloses that client request is received by the internet server which is also called content sever to access controlled files. Examiner considers the internet server is the access point of the network)*;

re-directing, by said AP, said access request to a local server *(col. 3, lines 27-29, Levergood discloses that content server initiates the authorization routine by redirecting the client's request to an authentication server)*;

transmitting an authentication request to said selected authentication server *(col. 3, lines 26-29, with respect to this limitation, Levergood discloses redirecting the client's request to an authentication server)* and

receiving a response to said authentication request from said selected authentication server *(col. 3, lines 29-33, Levergood discloses this limitation by the authentication server returns a response to qualified client)*.

Levergood does not specifically disclose associating unique data with an identifier of said client and storing a mapping of said association in said AP and generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client.

However, Stewart discloses associating unique data with an identifier of said client and storing a mapping of said association in said AP *(col. 2, lines 49-53, and access point associates user identification information to a network provider list. Unique data appears to be the network provider list)*.

Levergood and Stewart are analogous art because both applications teach the access control to a network or the Internet via a wire or wirelessly.

It would have been obvious to one of ordinary skilled in the art at the time of invention to further processing access request as disclosed by Levergood at an access point or an computing device as described in Stewart because it would provide various options to be authenticated to a network for a subscriber.

Jones discloses:

Hosting **a web page by said local server requesting that said client select an authentication server (AS)** *(page 5, [0059], wherein web server 114 corresponding with local server, authentication-invite web page corresponding with web page; [0060], web page can include a field for a user to select a service provider from among those available)* **and including said unique data and forwarding the web page to said client** *([0060], wherein SIP address, password, and/or other credentials correspond with unique data)*.

Levergood Stewart and Jones are analogous art because they are from the same field of endeavor of wireless communication access control.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify network access control as described by Levergood and add giving

user options to select a service provider as taught by Jones because it would provide mobile device user an other choice to connection to Internet while in the range of an hot spot.

Jones discloses hosting an authentication-invite webpage requesting client select an authentication server; however, Jones does not disclose generating the webpage, and forwarding said generated web page to said client.

Peiffer discloses **generating a webpage** *(par. [0058], the server is configured to recognize the SSID and generate a customized web resource A, based on the user's past behavior associated with the SSID)*.

Levergood, Stewart, Jones, and Peiffer are analogous art because they are from the same field of endeavor of network access controlling.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify hosting the authentication-invite web page stored at the server as described by Levergood in view of Jones to be generated at the server based receiving information as taught by Peiffer because it would provide customized web resource for client's request (see Peiffer, par. [0058], lines 14-19).

As per claim 3, Levergood discloses the method according to claim 1, further comprising: forwarding said identifier of said client from said local server; and generating said unique data for said client by said local server *(col. 3, lines 24-26, the internet server subjects the client to an authorization routine prior to issuing the SID. The SID considers as identifier, and the protected SID is the unique data of the server)*.

As per claim 4, Levergood discloses the method according to claim 1, further comprising:

retrieving, by said client, a re-directed URL having embedded data including a first digital signature, authentication parameters and said unique data and forwarding said re-directed URL to said AP *(col. 5, lines 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID. From lines 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16-bit ASCII string is considered as said unique data, and the authorized IP address is considered as said identifier. The browser forwards the request to a content server 120. As stated above, content server is considered as AP)*;

creating, by said AP, a second digital signature using said authentication parameters, said unique data and said identifier; comparing, by said AP, said first digital signature with said second digital signature *(col. 6, lines 5-8, the content server which is considered as AP tagged with SID. From lines 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The 16 character ASCII string is considered as said unique data, and the authorized IP address is considered as said identifier. The browser forwards the request to a content server 120)*;

determining, by said AP, if there is a match between said first digital signature and said second digital signature *(col. 6, lines 8-16, the SID's digital signature is compared against the digital signature computed)* and

performing, by said AP, one of granting network access and denying network access based on said match determination *(col. 6, lines 17-20, with respect to this limitation, Levergood discloses if the validation passes, the controlled resources will be granted to access)*.

As per claim 5, Levergood discloses the method according to claim 1, wherein said unique data includes a session ID and a randomized number *(col. 5, lines 54-65, the 16 character ASCII string that encodes 96 bits of SID data. Since it is encoded the data includes a randomized number)*.

As per claim 7, Levergood discloses the method according to claim 1, wherein the act of authenticating further comprises:

processing, by said AS, said authentication request, wherein said authentication request includes a session ID embedded in said authentication request *(col. 6, lines 27-65, client browser automatically sends a GET request to authentication server. Levergood discloses the embedded session ID in lines 62-63 by such as client IP address and password, as well as other information)*;

responding to said authentication request by forwarding to said client by said AS an authentication input page, said authentication input page including a request for authentication information *(col. 6, lines 40-49, with respect to this limitation, Levergood*

discloses authentication server sends a challenge responds which causes the client browser to prompt the user for credentials) and

receiving, by said AS, authentication credentials from said client, wherein said response to said authentication request forwarded to said client includes a re-direct header and a success code and associated information relevant to access of said network by said client *(col. 6, lines 58-67, and col. 7, lines 1-21, Levergood discloses this limitation by if user is authorized, the authentication server transmits a redirect response based on the tagged URL to client browser. An SID for an authorized user is appended)*.

As per claim 8, Levergood discloses the method according to claim 7, wherein the act of forwarding further comprises generating, by said AS, said success code and said associated information includes a first digital signature and authentication parameters *(col. 7, lines 14-20, an SID for an authorized user is appended. Levergood discloses The SID is sixteen character ASCII string and it contains a 32-bit digital signature in col. 5, lines 54-61. It is the as same as the SID Levergood mentioned in the rejection of claim 4)*.

As per claim 9, Levergood discloses the method according to claim 5, wherein said randomized number is one of a random number and a pseudo-random number *(col. 5, lines 54-65, the sixteen character ASCII string that encodes 96 bits of SID data. Since the SID is encoded the data it includes a random number or pseudo-random number)*.

As per claim 11, Steward discloses the method according to claim 1, wherein said AP and said local server are co-located *(col. 2, lines 63-66, the memory medium which may be a computer system can be comprised in the access point)*.

As per claim12, Levergood discloses the method according to claim 4, wherein said first and said second digital signatures are generated using one of a private key of said AS and a shared key between said AS and said local server *(col. 5, lines 61-65, the digital signature is a cryptographic hash that encrypted with secret key which is shared by the authentication and content servers)*.

As per claim 13, Levergood discloses the method according to claim 4, wherein said second digital signature is locally generated at said AP *(col. 6, lines 5-13, the first digital signature is compared against the second digital signature that computed by content server)*.

As per claim 34, Levergood discloses the method of claim 1, further comprising: at the authentication server, authenticating the client using the unique data, and forwarding said response to the client using a re-direct header, and including a digitally signed authentication message and authentication parameters corresponding to the unique data *(col. 7, lines 14-20, an SID for an authorized user is appended. The authentication server then transmits a redirect response to the client browser. Levergood discloses the SID is sixteen characters ASCII string and it contains a 32-bit digital signature, a 2-bit expiration date, a 22-bit user identifier and other information included in col. 5, lines 54-61)* and the access point receiving from the client according to the re-direct header the digitally signed authentication message and authentication

parameters *(col. 7, lines 14-20, content server receiving from the user according to the original URL directed header with an SID for the user is appended. Levergood discloses the SID is sixteen characters ASCII string and it contains a 22-bit user identifier and other information included in col. 5, lines 54-61).*

Stewart discloses correlating the authentication parameters with the mapped association data for determining access to the network *(col. 2, lines 60-67, and col. 3, lines 1-6, compare the received parameters with the mapped corresponding list to determine the appropriate network provider to access).*

AS per claim 36, Levergood discloses the method of claim 1, wherein said unique data comprises a session ID and a randomized number and further comprising: receiving, by said AP, a re-directed request from the client and including a digitally signed authentication message, an authentication parameter list, and said session ID, the digitally signed authentication message being generated using the randomized number, said session ID and said authentication parameter list, by said selected authentication server associated with the client *(col. 5, lines 22-65, user redirects URL get request at 100 in Fig. 2A contains an SID to content server. From lines 54 to 64, Levergood discloses that the preferred SID is a sixteen character string that encodes 96 bit of SID data. Since it is encoded it is involved in a randomized number. It includes a 32-bit digital signature, a 2-bit key identifier, and a 22-bit user identifier etc. The 22-bit user identifier is considered as authentication parameters. The URL directed to is the selected authentication server to the user).* Steward discloses and correlating the received digitally signed authentication message with the re-directed request for access

using the stored mapping data for controlling access by the client to the network *(col. 2, lines 49-66, access point receives the identification information for using a stored list to map for the controlling network access)*.

As per claim 41, Steward discloses the method according to claim 36, wherein said AP and said LS are co-located *(col. 2, lines 63-66, the memory medium which may be a computer system can be comprised in the access point)*.

9. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Neill in view of Manchala et al (US 2003/0079134, hereinafter Manchala).

As per claim 25, O'Neill discloses a system for controlling access to a network comprising:

a client *(fig. 11, and [0048], wherein mobile node MN 910 correspond with the client)*;

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client *(fig. 11,and [0048], wherein mobile node MN 910 correspond with the client, first Access Node FA 920 correspond with access point, AP; fig. 11, and [0049], wherein First Home Agent HA 930 correspond with Local server)*; and

an authentication server for performing an authentication process in response to a request from the client *(fig. 11,and [0048], send a message 906a to AAA, Authentication, Authorization and Accounting, server 905; wherein RADIUS*

access_request to the AAA system 905 correspond with authentication request); wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association *(fig. 11, and [0047], wherein binding table 933 correspond with associating, the information in MIP related to End Node 910 correspond with identifier of said client, and Host Home Address HoA correspond with Unique data)*;

the LS transmits the unique data to the client *(fig. 11, and [0050], lines 25-30, packet flow 960a from HA 930 to FA 920 includes packets destined for either the HoA 1 or HoA2 of the MN 910, wherein HoA 1 or HoA2 correspond with unique data)*;

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client *(fig. 11, [0047], lines 6-16, Authorization and Authentication system 905 enables the FA to authenticate the Mobile node 910; and [0048], wherein HoA correspond with unique data)*, the AP receiving authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation *(fig. 11, and page 7, [0047], lines 7-12, wherein binding table correspond with the mapped association data)*.

However, O'Neill discloses authorization and authentication system authenticates a mobile node; however, O'Neil does not disclose to provide a redirect header including a digitally signed authentication, and receiving the digitally signed retrieved re-directed URL.

Manchala discloses to provide **a redirect header including a digitally signed authentication** *(par. [0005]: request made to a server must contain HTTP headers containing the digital signature and a public key certificate that maps to the identity of the signer)*, **and receiving the digitally signed retrieved re-directed URL** *(par. [0005], a server receives the HTTP headers containing the digital signature and a public key certificate that maps to the identity of the signer)*.

O'Neill and Manchala are analogous art because they are from the same field of endeavor of wireless communication access control.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the authentication redirecting process as described by O'Neill and add the detail format of the redirecting header as taught by Manchala because it would provide accessing by using a mobile browser because the credential such as digital signature may be passed directly to another browser in order to convey permission to a resource (Manchala, par. [0005]).

As per claim 26, claim 25 is incorporated and O'Neill discloses:

wherein the network is a wireless local area network (WLAN) comprising the access point and local server *(fig. 11 and [0002], mobile communications; and [0048]-*

[0049], wherein first Access Node FA 920 correspond with access point, AP and First Home Agent HA 930 correspond with Local server).

10. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over O'Neill in view of Manchala, further in view of Jones and further in view of Peiffer.

As per claim 27, the system of claim 25 is incorporated and O'Neill in view of Manchala discloses a local server; however O'Neil in view of Manchala does not discloses generating a web page requesting that the client select an authentication server, and embeds the unique data in the web page for transmission to the client.

Jones discloses:

Hosting **a web page by said local server requesting that said client select an authentication server (AS)** *(page 5, [0059], wherein web server 114 corresponding with local server, authentication-invite web page corresponding with web page; [0060], web page can include a field for a user to select a service provider from among those available)* **and including said unique data and forwarding the web page to said client** *([0060], wherein SIP address, password, and/or other credentials correspond with unique data).*

O'Neill, Manchala and Jones are analogous art because they are from the same field of endeavor of wireless communication access control.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the verification process of a mobile node as described by O'Neill and add giving user options to select a service provider as taught by Jones because it would

provide mobile device user an other choice to connection to Internet while in the range of an hot spot.

Jones discloses hosting an authentication-invite webpage requesting client select an authentication server; however, Jones does not disclose generating the webpage, and forwarding said generated web page to said client.

Peiffer discloses **generating a webpage** *(par. [0058], the server is configured to recognize the SSID and generate a customized web resource A, based on the user's past behavior associated with the SSID)*.

O'Neill, Manchala, Jones, and Peiffer are analogous art because they are from the same field of endeavor of network access controlling.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify hosting the authentication-invite web page stored at the server as described by Jones to be generated at the server based receiving information as taught by Peiffer because it would provide customized web resource for client's request (see Peiffer, par. [0058], lines 14-19).

11. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Claxton et al (US Patent No. 7177839, hereinafter Claxton), and further in view of Yoshino et al (US 2003/0188117 A1, hereinafter Yoshino).

As per claim 42, Jones discloses a method for controlling network access, said method comprising:

receiving a request for network access *(fig. 3 and [0010], mobile station request to access the network)*;

re-directing said request via a message *(fig. 3 and [0010], wherein forwarding to the designated service provider correspond with re-directing request)*;

receiving a client identifier and unique data *(fig. 3 and [0060], wherein SIP address correspond with client identifier, password and/or other credentials correspond with unique data)*;

associating said unique data and said client identifier *(fig. 3 and [0062], wherein translation table correspond with associating)*;

receiving a re-directed universal resource locator included embedded information *(page 5, [0059], authentication-invite web page correspond with re-directed universal resource locator; [0060], wherein SIP address, password, and/or other credentials correspond with embedded data)*;

However, Jones does not explicitly disclose:

generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

comparing said local digital signature with a digital signature received in said embedded information;

granting network access if said local digital signature matches said digital signature received in said embedded information; and

deny network access if said local digital signature does not match said digital signature received in said embedded information.

Claxton discloses:

generating a local digital signature using said embedded information *(col. 51, lines 28-30, using public keys in their partner's certificate to regenerate a signature)*;

Claxton does not disclose generate digital signature using said association between said unique data and said client identifier;

Yoshino discloses generate digital signature using **said association between said unique data and said client identifier** (par. [0766], device executes the digital-signature generating processing by applying the device private key to the coupling data of received random number R and the device identifier; in light of the instant specification the association between unique data are the association between SID, and a random number etc in page 8, lines 3-6).

comparing said local digital signature with a digital signature received in said embedded information *(col. 51, lines 28-30, regenerate and compare signatures*;

granting network access if said local digital signature matches said digital signature received in said embedded information *(col. 51, lines 31-38, 56-65, if the account and SSL client certificates are valid, finally give access)*; and

deny network access if said local digital signature does not match said digital signature received in said embedded information *(col. 51, lines 31-38, 56-65, if the RM client is not authenticated, the request access denies)*.

Jones and Claxton are analogous art because they are from the same field of endeavor of electronic transaction system including an access point.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the allowing multiple service providers to serve users via a wireless local access network as described by Jones and add integrity verification to messages as taught by Claxton because it would achieve transport-level integrity and data privacy *(see Claxton, col. 51, lines 10-15)*.

Jones, Claxton, and Yoshino are analogous art because they are from the same field of endeavor of electronic transaction system including an access point.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify generating a signature by using the unique data a received information as described by Jones in view of Claxton and add generate the signature also based on other extra data information as taught by Yoshino because it would provide additional layer of security to prevent the invalid data accessing.

12. Claims 43 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Claxton, further in view of Yoshino and further in view of Chinnaswamy et al (US Publication No.: 2005/0114680).

As per claim 43, claim 42 is incorporated and Chinnaswamy discloses:

wherein said unique data comprises a session identifier and a random number *([0043], the message contains random number and session identifier)*.

Jones, Claxton, Yoshino, and Chinnaswamy are analogous art because they are from the same field of endeavor of electronic transaction system including an access point.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the allowing multiple service providers to serve users via a wireless local access network with integrity verification system as described by Jones in views of Claxton, and add data submitting for authentication including random number and Session ID as taught by Chinnaswamy because it would provide submitting details of the access control process.

As per claim 44, claim 42 is incorporated and Chinnaswamy discloses:

wherein said embedded information further comprises a session identifier and authentication parameters *([0043], the message contains random number and session identifier; wherein MAC_RAND and/or random number correspond with authentication parameters).*

Jones, Claxton, Yoshino, and Chinnaswamy are analogous art because they are from the same field of endeavor of electronic transaction system including an access point.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the allowing multiple service providers to serve users via a wireless local access network with integrity verification system as described by Jones in views of Claxton, and add data submitting for authentication including random number and Session ID as taught by Chinnaswamy because it would provide submitting details of the access control process.

Claims 45-47 are system claims corresponding to the methods claims 42-44 and therefore are rejected under the same reasons set forth in the rejections for claims 42-44.

Allowable Subject Matter

13. **Claims 28-33** objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JING SIMS whose telephone number is (571)270-7315. The examiner can normally be reached on 7:30am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JING SIMS/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437